

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

Криптографія
Лабораторна робота №3 (варіант 6)
Криптоаналіз афінної біграмної підстановки

Виконали:
студентки 3 курсу ФТІ
групи ФБ-93
Шрейдер Марія
Жембровська Олена

Перевірила:
Селюх П.В.

Мета роботи

Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиці.

Порядок виконання роботи

0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
1. Реалізувати підпрограми із необхідними математичними операціями: обчисленням оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв'язуванням лінійних порівнянь. При розв'язуванні порівнянь потрібно коректно обробляти випадок із декількома розв'язками, повертаючи їх усі.
2. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифртексту (за варіантом).
3. Перебрати можливі варіанти співставлення частих біграм мови та частих біграм шифртексту (розглядаючи пари біграм із п'яти найчастіших). Для кожного співставлення знайти можливі кандидати на ключ (a,b) шляхом розв'язання системи (1).
4. Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не є змістовним текстом російською мовою, відкинути цього кандидата.
5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.

Хід роботи

В ході роботи ми йшли за пунктами з «порядку виконання роботи».

Помітило, що в алфавіті, яких шифрувався тест були переставлені місцями букви «ы» та «ь».

Найчастіші біграми шифртексту

['ще', 'хе', 'чв', 'ле', 'цв']

Розпізнавач російської мови

Був обраний ентропійний критерій відбору змістовного тексту.

Для розшифрованих текстів по кожному зі знайдених ключів рахується ентропія тексту без перетинів та порівнюється зі значеннями, які були знайдені в першій лабораторній. Це приблизно від 4.4 до 4.5.

Повертається ключ, за яким ентропія розшифрованого тексту входить в даний проміжок.

Зашифрованный текст

ывлеюгзебшпещхщуйэвиывиюфгувхцубхщюнюжлепэшфмиьхдошбуднзегдшебоцвшуюгьпцвэ
шувкмзеиэбчиюндхщюасдбмонхегштгдэшжезьшемвошфысьмайыегыййййэшжеаекидщщежгь
деьцонгочвнюиюжвжудеьбюгьщесфвшвокуэйэящкщьюгочвнюлмшужеейцурпцвдэяхщаюьдеу
эвющэвдияйтвепцвчвлеюйщецыаешвэеяиктехщаэацизибвкмрйжуажййдекуштепэшфмздсу
гьвоцвайкзфштшхдуюиьйнюгдхацовойэрашеюияцияимюжцввджвяцэввлломоодмхщуйэм
юззопюзкнэщегбдсефвьхбжщенюцатщввэиегтеаехохтюйлдицзьхдшщюяьзщюоцвлеюосдлу
элзащавызийферддйомюиаыьепжмнюбжщцаешэзойтзэвзщупмюжьощаощвыжееююзьдеаей
юшдоездюйбпгьвиюэколпщхмоихсшфеэмлеотзомщйвхцывбжжебахизьщхйэашжеттфележебд
фюфпнюфмшуиэжяппшдгдщесдцжцвхеюцхеднвжееютбзийысддемилпмюзахшнюлллоюэпподй
шяюьхщужуиуцтабззлзьйопнбояшпиэщиамленйхдбднвнщлврпшилмиьадшахушайыэффппмю
цдсззезщадцьцихжшущфгбиэихеныжпбоцднесдегмаушйыктгдыйктийнвмоктздгидатаомтшл
вхеййрдияцшущюывмтшзюашнэьгозавюрдвджгмпиеэщеиэивдодзехатщйыэшзэшзунзщхеи
зчсдэайэхенвжьфжпсхгчплвжмвиртдэппшуртцюиэппедчидешорпдпвюбжлотвдюлофехщыдд
етеодайюяхрdbмлпнднелешхдошущазнибыутвднташебацэзьгордфесьаешзкнсднюятьд
аахмчвюцхеиовющежемпзькюжамюгьщцсбвдсчепзлепэшбмтвгоэвубюзмвппцинэзьэштапуи
эпхлеоенщнщрдэшлабмхтфуиуййаешэдэвлюцрпбжэщыдидсдщохилпийштгмищцвюбйощйапедм
лестгцатьчшбуэьгйцамиизавдкюяцрорпбдкьйомьщеаохдячвейчвэухвьхэерючежюшзюахмр
пййзхфйдыжецэзчящктьмоодььепюйййрйощююцдиеиатшхщнеэмьхгьощеююиьвдгивюьжшухе
хщкдэшжюяцлщлейдюйбпгьюййгдидндидбосдьдиараощаагюывмтвдцэзэяхщаййжтгпюфпэшя
иййхмлпияюцмахщмайвкмшувывбочвгййобуиэывзджюцгйбасдйэвюэасуяхуцбушфлпэь
вмхшоеяхрпдюцибофебаитвлпхлпэьуеюкюэлпбийэлпбинюфугьвоцвхестюцгдтэфйнезатшщ
авытдщааошумюжячаеаеаоодзтлояййысьюцсьмашайыьхлеяюсбфеюэшуйзлепрдюйкизолюуц
обуйюгктнвэииюдэяхщагююцхенедефепэлпсаййкияшбушзшзунтахаьыхдрпдэшчижеьюхиб
унюзьдесьюцаешфеюайвкмжгеэзчхаздхенехднвяшжесьвчаеяютвючсьцукммюфпэьхцхене
ешжпмюфгцвцвзщяшдыэжежуйэфгэзюайгыщоднвкгшвиьвчлпэьяьхэжмьхиьбшйыфпжягьмат
щаефмлестгцадьтцэьакгдйпгцэьдемимозщчртшгдцьэьшщузмонпамвикнсшувлонвиюовкмле
бпчвмвзьжемвшзгдяиампнлоппбообхдвхшнвшуялнюгьэабуохобхдзечадыегжеышхдктеаю
аирюунедмшчуудвайыэанвфупдэмчвмьщелеяймоюааачвэуопэьжеюэюаееыпхщаазяхзснгые
тепюхизьаелецуктпмзшршеьбюекгдьвтшщдчиубждгдхецкнвюиэвднвфузчшщдетадшимжйц
умюэщйюшйаэмтщвдеьйомюхебавахивлфеионвздокубтесаыдхшнвшуцуюрдцзшхмвлоцушц
шайюшдрддебочишукмжйпиуцфйжпщцоеидфгшйощемлмжгвдфвюаюобюаюьймвшжеэуяххарин
дшщэщгщчикгялнювамжфуощпйццмюегнещеегбдфюфпюйбпгьфпжйиэцвтбнещеегбмлещщзэяй
ьддьяецыфгсцфжтбшвяцвиошиалешщнвбчрийахиюкпммьшгяшулобжфгфиьжпптбшвиьййраы
ьнщеаощэшулопдищццаявяцбуиьэшхдвыбшпееыаебухтвдсдошийшщцыэщзщцймилмлежщощ
растиаэиюшщййзащеюиьцвмтшзлебджовшшхщужуиубэшулопдхомццвяйощвыявжявщэадо
щыштщкщфйыьжеуцщуыднвлеьэяхщабммоппмвппдюлмледшйидужижиженввииятпнзетечютд
юйбпгьчизднвепфйзшиакунэшщфпызайтьхиэианвзшушиорпбдпюцижефвчвйэгцлпнющецыа
еямтштазаощськммоцизилпбоодэаьдааощчвошюшдийрднпцвдщнюиадежпизвиьхсшрдехшу
йэтфппрюфпюцпмлпияшцоугьцааюфпэьавдтшфеоешпхэбонношиафпжяфпцвчвжьфждэлолвя
ьчвдодэайайыжевыоененезаиаразевыбвжйцулмлепешдерйхакииэяхщагютврюфпэшиацаыв
вюсюлоэуцвшэщйыаегюфпгьпднеизящсджпннхезефюфпящчвэвьхлммьдшоюьхиьрйрарежюг
ьщелекштьээмюфзнэцвсдмааеюиэисьмюцвэиубэфгшдещечйшвзкоусжээштеяииюфггшкею
ччэацапесьзецумозьхцоуоеуюмодшаййыхетеуиэижецэзчтэгчййыбозэгчййымааейшгюд
пюйбпгьишщхйэзьлвепцвсдчйыутвывяцбехдыиьхзавдссяобамшсдэанелезатэфйфщиээшне
жетштгдидчвяроеуюжйжпннтвшивлугцхлехштапэсбеелеяоодгджюубвюцдеюччшупнлмлеяеш
айыиалимьяшфгмючехйуышзкоусбшмазшбиьхзэзьйысьзьюауйжекюжмтшкдцьщхйэашцааюцв
мабзнэщегеюсюбжовшщцапейцщцвюлозьйычвййзаятдпэшьхлеяюсбеужищеегдьдэбоодфее
аоененетшкервтвэитзщанезчудйожецэзчкмючсджэзлрдяюнюиюэзмюсетпыжташенепхсшыщ
ьвчвнюлоизяцсбэапепешдийогдыйхедетамайвднвюдэяхщавооодбпртгьоецуппиачпковфн
дхшоедесшсдкюэьдэяцсдцааюцвэщфепэюцзасеяинэшзчуртэшсззеысдкюмвежцищемарцэл

утробы лотихоего родокутаный тьмой мирно нежил ся в постели пришло лето и ветер был летний и теплоедыхание мира неспешное и ленивое стоить лишь встать высунуть ся во кошко и тотчас

поймешь вот она начинается настоящая свобода и жизнь вот оно первое утро лета дуглас сполдинг двенадцати лет отроду только что открыл глаза как в теплую речку погрузился в предрассветную безмятежность он лежал в сводчатой комнате на четвертом этаже во всем городе не было башнивышей и оттого что он парил так высоко в воздухе вместе сиюньским ветром в нем ожидалась чудодейственная сила по ночам когда языки дубы клены сливались в одно беспокойное море дуглас кидал в него взглядом пронзавшимтьмуточномакакисегоднйавотздоровошепнул он впереди целое лето не счетное множество дней чуть неполкалендаря он уже видел себя много рук как божество шива из книжки про путешествия только поспевай рвать еще зеленые яблоки персики черные как ночь сливы его не вытащить из лесу из кустов из речки а как приятно будет померзнуть забравшись в заиндевелый ледник как весело жарить сывбабушкиной кухне за одностысячь юцплята пока задело раз в неделю ему позволяли ночевать в доме соседа в соседстве с палие города ители и младший братишка тома здесь в дедовской башне он в бегах потемной винтовой лестницы на самый верх и ложился спать в этой обители кудесника среди грома видений аспоза ранку когда даже молочники ещенезвякал бутылками на улицах он просыпался и приступал к заветному волшебству стоя в темноте у открытого окна он набрал полную грудь воздуха и изовсех сил дунул уличные фонари мигнули погасли точно свечки на черном мименинном пироге дуглас дунул еще и еще и в небесах зазвучали звезды дуглас улынулся и кнул пальцем там там там теперь тут тут тут тут в предутреннем тумане один за другим прорезались прямо углы домов зажигались огни далеко далеко на рассветной земле в другом зарилась целая вереница окон в семзевнутах в сем вставать огромный дом внизу ужил дедушка в нем айзубы из стакана дуглас немного подождет бабушка и прабабушка жарят оладьи с квасом и про несповсем коридорам теплый дух жареного теста и во всех комнатах встали и стрепенулись много численные тетки дяди двоюродные братья и сестры что сехались сюда погостить улица стариков просыпалась мисс Элен Лумис полковник Фрилей миссис Бенсли покашливает встаньте проглотите свои таблетки пошевеливайтесь мистер Джонас запрягайте лошадей выводите из сараев фургоны пора ехать за старьем по ту сторону уврага открылись свои драконы и глаза угрюмые собняки скоровнизу появляются на электрической зеленой машине двести старухи и покатят по утренним улицам приветственно махая каждой встречной собаке мистер Тридден бежит в трамвайное депо и в скорую по узким руслам мощеных улиц поплывет трамвай рассыпая вокруг жаркие синие искры Джонс Фанчарли вудмен вы готовы еще пнул дуглас улице детей готовы спросил он у бейсбольных мячей что мокли на росистых лужайках у пустых веревочных качелей что скачущая свисали с деревьев в мампаптом проснитесь тихонько прозвенели будильники гулко пробили часы на здании суда точно сел заброшенная егорукой с деревьев ввзметнулись птицы за пелидирижируя своим оркестром дуглас повелительно протянул руку к востоку и взошло солнце дуглас скрестил руки на груди и улынулся как на настоящий волшебник в тот тот тот тот тот думал он только приказали все повскакали все забегали отлично будет лето и он напоследок глядел горюдишкой кнулем у пальцами и распахнулись двери домов люди вышли на улицу лето тысяча девятьсот двадцать восьмого года началось в то утро проходя полужайке дуглас наткнулся на паутину невидимая нить коснулась его голба и неслышно олопнула и оттого пустячного случая он насторожился день будет не такой как в сен не такой еще и потому что бьют дни сотканые из одних запахов словно весь мир можно стянуть носом как воздух вдохнуть и выдохнуть так бы снял дуглас и его десятилетнему брату тому отцу когда вез их в машину за город а в другом и одного ворище от отца можно услышать каждый громик каждый шорох в селенной иныне дни хорошо пробовать на вкус а иныне на ощупь а бываюти такие когда есть все сразу вот например сегодня пахнет так будто в одну ночь там за холмами невесты откуда взялся огромный фруктовый сад в седомого горизонता кибагоухает в воздухе пахнет дождем но не небеню облачка того и гляди кто неведомый захочет в лесу покатать ишина дуглас во все глаза смотрел на плывущие мимо поля не тиса дом не пахнет ни дождем да и откуда бы разняблонь не тнитучик то там может хохотать в лесу авсетаки дуглас вздрогнул день этот какой то особенный машина остановилась в самом сердце тихого леса а ну ребята не баловать ся они подталкивали друг друга локтями хорошо папамальчики вылезли из машины захватили синие жестяные ведра и сойдя с пустынной проселочной дороги погрузились в запахи земли влажной от недавнего дождя и шипел скалозатец они всегда вьются в виноград как мальчишки в зокухне дуглас дуглас встrepенул ся опять витаешь в облаках скалозатец спустись на землю пойдем с нами хорошо

апаинигоуськомобрилолесувпередитотещрослыйиплечистыйзанималдугласапоследним
семенилкоротышка томподнялисьнаневысокийхолмипосмотреливдальвонтамуказалпаль
цемотецтамобитаютогромныеполетнемутихиеветрыинезримыеплывутвзеленыхглубинах
точнопризрачныекитыдугластглянулвтусторонуничегонеувиделипочувствовалсебяобм
анутымотецкакидедушкавечноговоритзагадкамиииивсетакидугласзатаилдыханиеиприс
лушалсячтотодолжнослучитьсяподумалоняужзнаюавотпапоротникназываетсявенерин
олосотецнеторопливошагалвпередсинееведропозвякивалоунеговрुкеаэточувствует
ионковырнулземлюноскомбашмакамиллионылеткопилсяэтотперегнойосеньзаосеньюпад
алилистьяпоказемлянесталатакоймягкойухтыяступаякакиндеецсказалтомсовсемнесл
ышнодугласпотрогалземлюноничегонеощутилонвсевремянастороженноприслушивалсям
ыокруженыдумалончтотослучитсяночтооностановилсывыхождаетытамчтотытакоемы
сленнокричалонтомиотецшлидальшепотихойподатливойземленасветенеткружеватоньш
енегромкосказалотецпоказалрукойвверхгделиствадеревьеввплеталасьвнебоилимож
етбытьнебовплеталосьвлиствувсеравноулыбнулсяотецвсезтокружевазеленыеиголубы
евсмотритехорошенькоиувидителесплететихсловногудящийстанокотецстоялуверен
нопохозяйскиирассказывалимвсякуювсичинулегкоисвободноневыбираясловчастоонис
амсмеялсясвоимрассказамиотэтогоонитеклиещесвободнеехорошоприслушаепослушать
тишинуговорилонпотомучтотогдадаетсяуслышатькакноситсяввоздухепыльцаполевых
цветовавоздухтакигудитпчеламидадатакигудитавотслышитетамзадеревьямиводопада
мльетсяптичьещебетаньевогсейчасдумалдугласвотонужеблизкоаяещеневижусовсемб
лизкорядомдикийвиноградсказалотецнамповезлосмотритеканенадоахнулпросебядугл
аснотомииотецнаклонилисьипогрузилирукившуршащийкустчарырассеялисьтопугающееи
грозноечтоподкрадывалосьблизилосьготовобылоринутьсяипотрястиегодушуисчезлоо
пустошенныйрастерянныйдугласупалнаколенипальцыегоушлиглубоковзеленуютеньвы
нырнулиоблагренныеалымсокомсловноонврезаллесножомисунулрукивоткрытуюранумал
ьчикизавтракатьведрачутьнедоверхунаполненыдикиимвиноградомилеснойземляникойв
округгудятпчелыэтовосенепчелыцелыймиртихонькомурлычетсвоюпесенкуговоритот
ецаонисидятназамшеломстволеупавшегодереважуютсандвичиипытаютсяслушатьлескак
слушаефонотецчутьпосмеиваясьискосапоглядываетнадугласахотелбылочтотосказать
нопромолчалоткусилещекусоксандвичаизадумалсяхлебсветчинойвлесунетчтодомавк
уссовсемдругойверноостреечтолимятойотдаетсмолойаужаппетиткакразыгрываетсяду
гласпересталжеватьипотрогалязыкомхлебиветчинунетнетобыкновенныйсандвичтомки
внулпродолжаяжеватьяпонимаюпапведьужепочтислучилосьдумаетдугласнезнаючтоэто
нонобольшуеепрямогромдаеетчтотоегоспугнулогдежеонотеперьопятьушловтоткуст
нетгдетозамнойнетнетздесьтутрядомдугласисподтишкапощупалсвойживотоноещеверн
етсянадотольконемножкоподождатьбольнонебудетяужзнаюнезатемонокомнепридетноз
ачемжезачема

Висновки: в ході лабораторної роботи дослідили та реалізували метод розшифрування шифру афінної підстановки біграм. А також дізналися про критерії відбору змістовних текстів і реалізували один з них.